Claims 1-40 (Cancelled.)

41. (Currently Amended) A method for remotely monitoring each of a plurality of network intrusion protection devices with a remote monitoring center under control by a service provider servicing the intrusion protection requirements of a plurality of customers, ~~wherein the remote monitoring center operates at a location other than a site of any one of the customers~~, comprising the steps of:

receiving at the remote monitoring center a first transmission comprising a first identification number and a network address associated with one of a plurality of network intrusion prevention ~~communication~~ devices monitored by the remote monitoring center which operates at a location other than a site of any one of the customers, each network intrusion prevention ~~communication~~ device positioned in-line ~~with~~ and between a computer network controlled by one of the customers and a distributed computer network that is not controlled by the customers, each network intrusion prevention ~~communication~~ device operative to block a communication from passing to the corresponding computer network via the distributed computer network by terminating the communication based on a determination that the communication represents a security risk to at least one of the computers coupled to the computer network, each network intrusion prevention device operative to make the determination that the communication represents a security risk independently after being configured and without control from the remote monitoring center, each network intrusion prevention device comprising a firewall, an intrusion detector, and a remote monitoring controller communication module, wherein the remote monitoring controller communication module is operatively coupled to the remote monitoring center;

storing the identification number and network address for the network intrusion prevention ~~communication~~ device in a database at the remote monitoring center;

receiving at the remote monitoring center a second identification number during a second transmission from the network intrusion prevention ~~communication~~ device;

comparing the second identification number with the first identification number at the remote monitoring center and, in response to a match between the first identification number and second identification number, identifying a plurality of security policy options that are selectable by the network intrusion prevention ~~communication~~ device;

generating a configuration file with the remote monitoring center in response to selection of at least one of the security policy options by the network intrusion prevention ~~communication~~ device, the configuration file governing the intrusion protection operation for the network intrusion prevention ~~communication~~ device;

transmitting the configuration file from the remote monitoring center to configure the network intrusion prevention ~~communication~~ device;

monitoring the network intrusion prevention ~~communication~~ device by the remote monitoring center for issuance of an alert signal issued by the network intrusion prevention ~~communication~~ device in response to a determination that the communication represents a security risk to at least one of the computers coupled to the computer network;

receiving the alert signal at the remote monitoring center; and

assigning the alert signal an order and taking responsive action at the remote monitoring center based upon the assigned order.

42. (Currently Amended) The method of claim 41, further comprising the step of storing the alert signal into another database connected to the remote monitoring center, wherein servicing the protection requirements of a plurality of customers comprises monitoring each of the plurality of network intrusion prevention ~~communication~~ devices for generation of the alert signal.

43. (Currently Amended) The method of claim 41, further comprising the step of:

receiving at the remote monitoring center status information from one of the network intrusion prevention ~~communication~~ devices;

recording the status information in the database; and

determining whether the network intrusion prevention ~~communication~~ device meets a plurality of operational requirements based upon the status information.

[The Remainder of this page has been intentionally left blank.]

44. (Currently Amended) The method of claim 41, further comprising the steps of:

receiving at the remote monitoring center a plurality of diagnostic variables from one of the network intrusion prevention ~~communication~~ devices; and

determining whether the network intrusion prevention ~~communication~~ device is functioning properly based on the diagnostic variables.

45. (Currently Amended) The method of claim 41, further comprising the steps of:

receiving at the remote monitoring center status information from one of the network intrusion prevention ~~communication~~ devices;

determining whether the network intrusion prevention ~~communication~~ device requires a software patch based upon the status information; and

transmitting the software patch to the network intrusion prevention ~~communication~~ device in response to determining the network intrusion prevention ~~communication~~ device requires the software patch.

46. (Currently Amended) The method of claim 41, further comprising the steps of:

receiving at the remote monitoring center a configuration complete signal;

performing a vulnerability analysis on one of the network intrusion prevention ~~communication~~ devices; and

evaluating the results of the vulnerability analysis.

[The Remainder of this page has been intentionally left blank.]

47. (Currently Amended) A method for remotely monitoring a plurality of network intrusion prevention ~~communication~~ devices based on operations of a remote monitoring center managed by a service provider, ~~each communication device positioned in-line with a computer network under control of one of a plurality of customers and a distributed computer network that is not under control of the customers,~~ comprising the steps of:

presenting security policy options with the remote monitoring center, the security policy options selectable by each of the network intrusion prevention ~~communication~~ devices, each network intrusion prevention communication device positioned in-line and between a computer network under control of one of a plurality of customers and a distributed computer network that is not under control of the customers;

generating a configuration file with the remote monitoring center in response to selection of the security policy options by each of the network intrusion prevention ~~communication~~ devices;

transmitting the configuration file from the remote monitoring center to configure the network intrusion prevention ~~communication~~ devices, each network intrusion prevention ~~communication~~ device operative to process a communication carried by the distributed computer network and intended for delivery to a computer coupled to a corresponding one of the computer networks to determine whether the communication represents a security risk to the computer network in accordance with the configuration file, each network intrusion prevention device operative to determine whether the communication represents a security risk independently after being configured and without control from the remote monitoring center, the network intrusion prevention ~~communication~~ device further operative to issue an alert signal and to terminate the communication in response to a determination that the communication represents a security risk, each network intrusion prevention device comprising a firewall, an intrusion detector, and a remote monitoring controller communication module, the remote monitoring controller communication module coupled to the remote monitoring center;

monitoring the network intrusion prevention ~~communication~~ devices with the remote monitoring center to detect an issuance of the alert signal from one of the network intrusion prevention ~~communication~~ devices;

receiving the alert signal with the remote monitoring center; and

forwarding the alert signal to a remote agent associated with the service provider, wherein the alert signal provides an advisory of the security risk faced by the network intrusion prevention ~~communication~~ device that issued the alert signal.

48. (Previously Presented) The method of claim 47, further comprising the steps of:

assigning a priority to the alert signal upon receipt of the alert signal at the remote monitoring center; and

forwarding the alert signal to the remote agent according to the assigned priority.

49. (Currently Amended) The method of claim 47, further comprising the steps of:

receiving the alert signal with the remote agent;

determining an appropriate resolution to address the alert signal; and

sending a message comprising the resolution to a particular one of the customers associated with the network intrusion prevention ~~communication~~ device that issued the alert signal.

50. (Currently Amended) The method of claim 47, further comprising the steps of:

prior to displaying security policy options, receiving a wake-up signal from one of the network intrusion prevention ~~communication~~ devices at the remote monitoring center; and

in response to the wake-up signal, transmitting the configuration file form the remote monitoring center to the network intrusion prevention ~~communication~~ device.

51. (Currently Amended) The method of claim 47, further comprising the step of:

receiving a first identification number and a network address at the remote monitoring center from one of the network intrusion prevention ~~communication~~ devices; and

recording the first identification number and the network address in a database connected to the remote monitoring center.

52. (Currently Amended) The method of claim 47, further comprising the step of:

receiving at the remote monitoring center status information from one of the network intrusion prevention ~~communication~~ devices;

recording the status information in a database; and

determining whether the network intrusion prevention ~~communication~~ device meets a plurality of operational requirements based upon the status information.

53. (Currently Amended) The method of claim 47, further comprising the steps of:

receiving at the remote monitoring center a plurality of diagnostic variables from one of the network intrusion prevention ~~communication~~ devices; and

determining whether the network intrusion prevention ~~communication~~ device is functioning properly based on the diagnostic variables.

54. (Currently Amended) The method of claim 47, further comprising the steps of:

receiving at the remote monitoring center status information from one of the network intrusion prevention ~~communication~~ devices;

determining whether the network intrusion prevention ~~communication~~ device requires a software patch based upon the status information; and

transmitting the software patch to the network intrusion prevention ~~communication~~ device in response to determining that the network intrusion prevention ~~communication~~ device requires the software patch.

55. (Currently Amended) The method of claim 47, further comprising the steps of:

responsive to configuration of one of the network intrusion prevention ~~communication~~ devices, performing a vulnerability analysis for the network intrusion prevention ~~communication~~ device; and

determining whether the network intrusion prevention ~~communication~~ device failed the vulnerability analysis.

Claims 56-60 (Cancelled.)

[The Remainder of this page has been intentionally left blank.]

61. (Currently Amended) A system for remotely monitoring the security status of a plurality of computer networks, each computer network associated with one of a plurality of entities, comprising:

a plurality of network intrusion prevention ~~communication~~ devices, each network intrusion prevention ~~communication~~ device coupled in-line ~~with~~ and between one of the computer networks associated with a particular one of the entities and a distributed computer network that is not associated with any of the entities,

wherein each network intrusion prevention ~~communication~~ device is operative to process a communication carried by the distributed computer network and intended for delivery to a computer coupled to the corresponding computer network to determine whether the communication represents a security risk to the computer network, and

wherein each network intrusion prevention ~~communication~~ device is further operative to block the communication from passage to the computer network by terminating the communication and to transmit an alert signal via the distributed computer network in response to a determination by the network intrusion prevention ~~communication~~ device that the communication represents a security risk, each network intrusion prevention device operative to make the determination that the communication represents a security risk independently after being configured and without control of a remote monitoring center, each network intrusion prevention device comprising a firewall, an intrusion detector, and a remote monitoring controller communication module, the remote monitoring controller communication module coupled to the remote monitoring center; and

[[a]] the remote monitoring center operated on behalf of the entities by a service provider, the remote monitoring center coupled to the distributed computer network, remotely located from each of the computer networks, and operative to monitor the security status of each one of the plurality of computer networks based upon status information transmitted by the network intrusion prevention ~~communication~~ devices for the computer networks, the remote monitoring center responsive to receipt of the alert signal transmitted by any one of the network intrusion prevention ~~communication~~ devices to complete an analysis of the alert signal and to take a responsive action based on the analysis of the alert signal.

62. (Currently Amended) The system of Claim 61, wherein the remote monitoring center comprises:

one or more remote agent personnel for evaluating the alert signal;

a database for storing alert information presented by the alert signal;

a server maintaining security configuration options for each of the network intrusion prevention ~~communication~~ devices;

a controller for permitting access to the network intrusion prevention ~~communication~~ device security options based upon a comparison of identification information associated with one of network intrusion prevention ~~communication~~ devices to identification information stored in the database, and for transmitting a configuration file to the network intrusion prevention ~~communication~~ device in response to a configuration request made by the network intrusion prevention ~~communication~~ device; and

a monitoring engine for receiving the alert signal and recording information about the alert signal in the database, and for forwarding the alert signal to the one or more remote agent personnel.

63. (Currently Amended) The system of claim 62, wherein each agent personnel is under control of the service provider while each network intrusion prevention ~~communication~~ device is under control of one of the entities subscribing to a network security monitoring service sponsored by the service provider.

64. (Currently Amended) The system of claim 62, wherein one of the agent personnel recommends a responsive action to take in reply to the alert signal, the responsive action presented to the entity associated with the network intrusion prevention ~~communication~~ device that issued the alert signal, the responsive action delivered via one of a Web server, an e-mail message, a telephone, and a pager.

65. (Currently Amended) The system of claim 61, wherein each network intrusion prevention ~~communication~~ device comprises:

an intrusion detector, positioned between the computer network and the distributed computer network, for receiving the network intrusion prevention ~~communication~~ from the distributed computer network and processing the communication to determine whether the communication represents a security risk;

a processor operative to determine a network address for the network intrusion prevention ~~communication~~ device; and

a transmitter for sending the wake-up signal comprising the network address to the remote monitoring center via the distributed computer network, the transmitter further operative to send the alert signal in response to a determination by the intrusion detector that the communication represents a security risk.

Claims 66-70 (Cancelled.)

[The Remainder of this page has been intentionally left blank.]